Efficient and economic five-party quantum state sharing of an arbitrary m-qubit state

Yu-Bo Sheng,[1,2,3] Fu-Guo Deng,[1,2,3,4*] and Hong-Yu Zhou[1,2,3]
[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, China*
[3] *Beijing Radiation Center, Beijing 100875, China*
[4] *Department of Physics, Applied Optics Beijing Area Major Laboratory, Beijing Normal University, Beijing 100875, China*
(Dated: May 4, 2010)

We present an efficient and economic scheme for five-party quantum state sharing of an arbitrary m-qubit state with $2m$ three-particle Greenberger-Horne-Zeilinger (GHZ) states and three-particle GHZ-state measurements. It is more convenient than other schemes as it only resorts to three-particle GHZ states and three-particle joint measurement, not five-particle entanglements and five-particle joint measurements. Moreover, this symmetric scheme is in principle secure even though the number of the dishonest agents is more than one. Its total efficiency approaches the maximal value.

PACS numbers: 03.67.Hk Quantum communication - 03.67.Dd Quantum cryptography

I. INTRODUCTION

In a secret sharing, a boss, say Alice wants to send a secret message M_A to her two agents, say Bob and Charlie who are far away from Alice. Alice suspects that one of the two agents may be dishonest and the dishonest one will do harm to her benefit if he can obtain the secret message independently. Unfortunately, Alice does not know who the dishonest agent is. Alice believes that the honest agent can prevent the dishonest one from destroying her benefit if they act in concert. In classical secret sharing crypto-system [1], Alice splits her secret message M_A into two pieces M_B and M_C, and then sends them to Bob and Charlie, respectively. When Bob and Charlie cooperate, they can read out the message $M_A = M_B \oplus M_C$; otherwise, none can obtain a useful information about the secret message. As classical signals can be copied fully and freely, it is in principle impossible for Alice to transmit her secret message directly to her agents with only classical physics. An alternative is that Alice first creates a private key with each of the agents, and then encrypts the secret message with one-time pad crypto-system before she sends it to her agents. At present, quantum key distribution (QKD) [2–6] provides a secure way for generating a private key between two authorized parties. With some private keys, the three parties can share the secret message M_A securely. Quantum secure direct communication [7–10] in principle supplies a secure way for transmitting the messages M_B and M_C directly with quantum memory.

Quantum secret sharing (QSS) is the generalization of classical secret sharing [1] into quantum scenario. There are two main goals in QSS. One is used to share a private key. The other is used to share a quantum information, i.e., an unknown state. In 1999, Hillery, Bužek and Berthiaume (HBB) [11] proposed an original QSS scheme for sharing a private key with entangled three-particle Greenberger-Horne-Zeilinger (GHZ) states. Subsequently, Karlsson, Koashi and Imoto [12] presented a QSS scheme for creating a private key among three parties with two-particle entangled states. Xiao et al. [13] generalized the HBB QSS scheme to the case with N agents and also gave out two ways for improving the efficiency of qubits in the QSS scheme [11]. Now, there are a great number of QSS schemes for sharing a private key, including the schemes [14–21] with entangled quantum systems and those [22–27] with single photons. When QSS is used to share an unknown state, it has to resort to quantum entanglement [28–41]. In HBB QSS scheme [11], the authors presented a scheme for controlled teleporation of an arbitrary qubit, in which the receiver can recover an unknown state only when he cooperate with the controllers. In 1999, Cleve, Gottesman and Lo [28] proposed a scheme for sharing a quantum secret with three-dimensional quantum states. In 2004, Lance et al. named the branch of quantum secret sharing for quantum information "quantum-state sharing" (QSTS) [29]. In essence, QSTS equals to controlled teleporation [31–34]. In 2004, Li et al.[30] introduced a scheme for sharing an unknown single qubit with a multipartite joint measurement (i.e., multipartite GHZ-state measurement). In 2005, Deng et al. proposed a symmetric scheme for controlled teleportation of an arbitrary two-particle state with a GHZ-state quantum channel [31] and a QSTS scheme for sharing an arbitrary two-particle state with a Bell-state quantum channel [32]. In 2006, Li et al. [33] proposed an efficient symmetric multiparty quantum state sharing scheme for an arbitrary m-qubit state with a GHZ-state quantum channel. Also, they generalized this scheme to the case for sharing an unknown d-dimensional quantum system [34]. In 2006, Deng et al.

*Electronic mail: fgdeng@bnu.edu.cn

[40] proposed a circular QSTS scheme for sharing an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements. Now the models for sharing an unknown state with a non-maximally entangled quantum channel are studied by some groups [35–39].

Although there are some QSTS schemes for sharing a single qubit or an m-qubit quantum system, they are either not economic or insecure for the case with two dishonest agents. For instance, the schemes in Refs. [11, 13, 31–38] require a five-particle GHZ-state quantum channel for sharing a unknown single-qubit state when they are used for five-party quantum state sharing, that in Ref. [30] requires five-particle GHZ-state measurements, and the schemes in Refs. [40, 41] cannot prevent two dishonest agents from eavesdropping the message freely when they cooperate. In this paper, we will present an efficient and economic five-party QSTS scheme for sharing an arbitrary m-qubit state. It only resorts to a three-particle GHZ-state quantum channel and three-particle GHZ-state measurements, not a five-particle GHZ-state quantum channel [31] or five-particle GHZ-state joint measurements [30]. Moreover, this scheme is secure if the number of the dishonest agents is more than one (no more than three). Except for the sender Alice, all the agents need only to take m single-particle measurements on their particles for controlling the receiver to reconstruct the unknown quantum state. It is more convenient than others in a practical application. As almost all the quantum resource can be used to sharing the quantum information and the classical information exchanged is minimal, the total efficiency in this scheme approaches the maximal value.

II. ECONOMIC FIVE-PARTY QSTS SCHEME FOR SHARING A SINGLE-QUBIT STATE

For three-particle maximally entangled quantum systems, the eight GHZ states can be written as follows:

$$|\Psi_0\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}, \quad (1)$$

$$|\Psi_1\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)_{ABC}, \quad (2)$$

$$|\Psi_2\rangle_{ABC} = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)_{ABC}, \quad (3)$$

$$|\Psi_3\rangle_{ABC} = \frac{1}{\sqrt{2}}(|001\rangle - |110\rangle)_{ABC}, \quad (4)$$

$$|\Psi_4\rangle_{ABC} = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{ABC}, \quad (5)$$

$$|\Psi_5\rangle_{ABC} = \frac{1}{\sqrt{2}}(|010\rangle - |101\rangle)_{ABC}, \quad (6)$$

$$|\Psi_6\rangle_{ABC} = \frac{1}{\sqrt{2}}(|011\rangle + |100\rangle)_{ABC}, \quad (7)$$

$$|\Psi_7\rangle_{ABC} = \frac{1}{\sqrt{2}}(|011\rangle - |100\rangle)_{ABC}, \quad (8)$$

where $|0\rangle$ and $|1\rangle$ are the two eigenstates of the Pauli operator σ_z, called it Z measuring basis (MB) (for example, the polarization of photons along the z-direction, and $|0\rangle$ and $|1\rangle$ represent the horizontal and the vertical polarizations).

For sharing an arbitrary qubit x which is in the state $|\chi\rangle_x = \alpha|0\rangle + \beta|1\rangle$ among the five parties, say Alice, Bob_i ($i = 1, 2, 3$), and Charlie, the boss Alice first shares two three-particle GHZ states $|\Psi_0\rangle$ with her four agents (see Fig.1). That is, Alice shares a three-particle GHZ state $|\Psi_0\rangle_{A_1B_1B_2}$ with Bob_1 and Bob_2, and shares another three-particle GHZ state $|\Psi_0\rangle_{A_2B_3C}$ with Bob_3 and Charlie. Alice keeps the particles A_1 and A_2. Alice can share securely the GHZ states with her agents by using the decoy-photon technique [42]. In detail, when Alice wants to share a sequence of three-particle GHZ states with her agents Bob_1 and Bob_2 (or Bob_3 and Charlie), she prepares some decoy photons which are randomly in one of the four states $\{|0\rangle, |1\rangle, |+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ and then inserts them in the two sequences of the GHZ-state particles. Alice sends the two sequences to her two agents, respectively. Alice and her agents can exploit the decoy photons to check the security of the transmission [43].

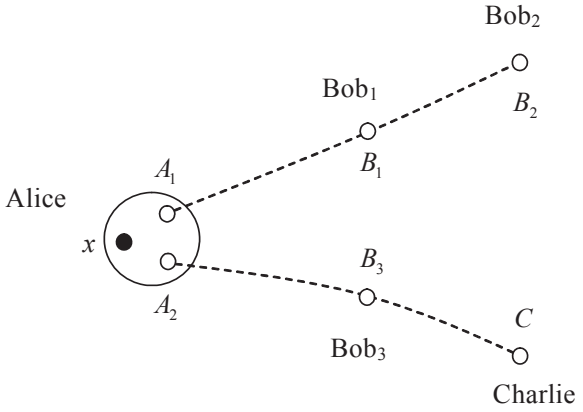

FIG. 1: The principle of this QSTS scheme. The three particles linked with the dashed lines are in the GHZ state $|\Psi_0\rangle$. The round represents a three-particle GHZ-state measurement.

After setting up the quantum channel (two sequences of GHZ states) with her agents, Alice can transfer her quantum information (the unknown state) to the particles controlled by all the agents. In detail, Alice performs a three-particle GHZ-state measurement on the particles x, A_1, and A_2, and the quantum information of the unknown qubit x will be transferred into the subsystem composed of the four particles B_1, B_2, B_3, and C. The four agents can extract the quantum information with cooperation as the state of the composite quantum system comprising the seven particles x, A_1, A_2, B_1, B_2, B_3, and C can be written as

$$
\begin{aligned}
|\Phi\rangle_s &\equiv |\chi\rangle_x \otimes |\Psi_0\rangle_{A_1B_1B_2} \otimes |\Psi_0\rangle_{A_2B_3C} \\
&= (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{A_1B_1B_2} \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{A_2B_3C} \\
&= \frac{1}{2\sqrt{2}}[|\Psi_0\rangle_{xA_1A_2}(\alpha|00\rangle_{B_1B_2}|00\rangle_{B_3C} + \beta|11\rangle_{B_1B_2}|11\rangle_{B_3C}) + |\Psi_1\rangle_{xA_1A_2}(\alpha|00\rangle_{B_1B_2}|00\rangle_{B_3C} - \beta|11\rangle_{B_1B_2}|11\rangle_{B_3C}) \\
&\quad + |\Psi_2\rangle_{xA_1A_2}(\alpha|00\rangle_{B_1B_2}|11\rangle_{B_3C} + \beta|11\rangle_{B_1B_2}|00\rangle_{B_3C}) + |\Psi_3\rangle_{xA_1A_2}(\alpha|00\rangle_{B_1B_2}|11\rangle_{B_3C} - \beta|11\rangle_{B_1B_2}|00\rangle_{B_3C}) \\
&\quad + |\Psi_4\rangle_{xA_1A_2}(\beta|00\rangle_{B_1B_2}|11\rangle_{B_3C} + \alpha|11\rangle_{B_1B_2}|00\rangle_{B_3C}) - |\Psi_5\rangle_{xA_1A_2}(\beta|00\rangle_{B_1B_2}|11\rangle_{B_3C} - \alpha|11\rangle_{B_1B_2}|00\rangle_{B_3C}) \\
&\quad + |\Psi_6\rangle_{xA_1A_2}(\beta|00\rangle_{B_1B_2}|00\rangle_{B_3C} + \alpha|11\rangle_{B_1B_2}|11\rangle_{B_3C}) - |\Psi_7\rangle_{xA_1A_2}(\beta|00\rangle_{B_1B_2}|00\rangle_{B_3C} - \alpha|11\rangle_{B_1B_2}|11\rangle_{B_3C})].
\end{aligned} \tag{9}
$$

When Alice gets the outcome $|\Psi_0\rangle_{xA_1A_2}$, the subsystem composed of the particles controlled by all the four agents collapses to the state $\phi_0 = \alpha|00\rangle_{B_1B_2}|00\rangle_{B_3C} + \beta|11\rangle_{B_1B_2}|11\rangle_{B_3C}$. The three controllers Bob_1, Bob_2, and Bob_3 take a measurement with the basis X on their particles B_1, B_2, and B_3, respectively. If the number of the controllers who obtain the outcome $|+x\rangle$ is even, the particle C will collapse to the state $\alpha|0\rangle + \beta|1\rangle$ and Charlie needs doing nothing on his particle for recovering the originally unknown state $|\chi\rangle$; otherwise, the state of the particle C becomes $\alpha|0\rangle - \beta|1\rangle$ and Charlie needs performing a phase-flip operation $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ on the particle C to recover the unknown state $|\chi\rangle$.

$$
\begin{aligned}
\phi_0 &= \alpha|00\rangle_{B_1B_2}|00\rangle_{B_3C} + \beta|11\rangle_{B_1B_2}|11\rangle_{B_3C} \\
&= \frac{1}{2\sqrt{2}}[(|+x\rangle|+x\rangle|+x\rangle + |+x\rangle|-x\rangle|-x\rangle + |-x\rangle|+x\rangle|-x\rangle + |-x\rangle|-x\rangle|+x\rangle)_{B_1B_2B_3}(\alpha|0\rangle + \beta|1\rangle)_C \\
&\quad + (|+x\rangle|+x\rangle|-x\rangle + |+x\rangle|-x\rangle|+x\rangle + |-x\rangle|+x\rangle|+x\rangle + |-x\rangle|-x\rangle|-x\rangle)_{B_1B_2B_3}(\alpha|0\rangle - \beta|1\rangle)_C].
\end{aligned} \tag{10}
$$

TABLE I: The relation between the unitary operations used for recovering the unknown state and the outcomes obtained by Alice, Bob_1, Bob_2, and Bob_3.

$V_{xA_1A_2}$	P_{total}	ϕ_C	operations
0	+	$\alpha\|0\rangle + \beta\|1\rangle$	I
0	−	$\alpha\|0\rangle - \beta\|1\rangle$	σ_z
1	+	$\beta\|0\rangle + \alpha\|1\rangle$	σ_x
1	−	$\beta\|0\rangle - \alpha\|1\rangle$	$i\sigma_y$

When Alice gets the other outcomes with GHZ-state measurements on the particles x, A_1, and A_2, the relation between the outcomes obtained by the controllers and the unitary operations needed for recovering the unknown state $|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$ is shown in Table I. Here $V_{xA_1A_2}$ is the value of the outcome obtained by Alice. We code the states $\{|\Psi_0\rangle_{xA_1A_2}, |\Psi_1\rangle_{xA_1A_2}, |\Psi_4\rangle_{xA_1A_2}, |\Psi_5\rangle_{xA_1A_2}\}$ as 0 and the states $\{|\Psi_2\rangle_{xA_1A_2}, |\Psi_3\rangle_{xA_1A_2}, |\Psi_6\rangle_{xA_1A_2}, |\Psi_7\rangle_{xA_1A_2}\}$ as 1. For example, $V_{xA_1A_2} = 0$ if Alice gets the outcome $|\Psi_0\rangle_{xA_1A_2}$ with her GHZ-state measurement. In this table, $P_{total} = P_A P_{B_1} P_{B_2} P_{B_3}$. Here P_A, P_{B_1}, P_{B_2}, and P_{B_3} are the parities of the outcomes obtained by Alice, Bob_1, Bob_2, and Bob_3, respectively. Similar to Refs. [31–33], we code the parities of the states $\{|\Psi_0\rangle_{xA_1A_2}, |\Psi_2\rangle_{xA_1A_2}, |\Psi_4\rangle_{xA_1A_2}, |\Psi_6\rangle_{xA_1A_2}\}$ as + and $\{|\Psi_1\rangle_{xA_1A_2}, |\Psi_3\rangle_{xA_1A_2}, |\Psi_5\rangle_{xA_1A_2}, |\Psi_7\rangle_{xA_1A_2}\}$ as −. For the outcomes obtained by the controllers Bob_1, Bob_2, and Bob_3, the state $|+x\rangle$ represents the parity + and the state $|-x\rangle$ represents the parity −. ϕ_C is the state of the particle C controlled by Charlie before the unitary operation is done. σ_z, σ_x, and σ_y are the Pauli operations, i.e.,

$$
\begin{aligned}
I &= |0\rangle\langle 0| + |1\rangle\langle 1|, && (11)\\
\sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1|, && (12)\\
\sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0|, && (13)\\
i\sigma_y &= |0\rangle\langle 1| - |1\rangle\langle 0|. && (14)
\end{aligned}
$$

From Table I, one can see that Alice need only publish two bits of classical information about her three-particle GHZ-state measurement for her agents to recover the unknown state, not three bits of classical information. Each of the controllers should announce one bit of classical information about the outcome of the measurement with

the basis X, and the receiver Charlie can recover the unknown state $|\chi\rangle$ with a unitary operation.

III. ECONOMIC FIVE-PARTY QSTS SCHEME FOR SHARING AN ARBITRARY m-QUBIT STATE

It is straightforward to generalize this five-party QSTS scheme to the case for sharing an arbitrary m-qubit state. Same as Ref. [33], an m-qubit state can be described as

$$|\xi\rangle_u = \sum_{ij\ldots k} a_{\underbrace{ij\ldots k}_{m}} |\underbrace{ij\ldots k}_{m}\rangle_{x_1x_2\ldots x_m}, \qquad (15)$$

where $i, j, \ldots, k \in \{0, 1\}$, and $x_1, x_2, \ldots$, and x_m are the m particles in the unknown state. For sharing m-qubit state $|\xi\rangle_u$, Alice should share at least m three-particle GHZ states $|\Psi_0\rangle$ with each two of her agents, i.e., set up a quantum channel with $2m$ GHZ states securely. The state of the composite quantum system composed of the particles in the unknown m-qubit state and the GHZ states can be written as

$$|\Psi\rangle \equiv (\sum_{ij\ldots k} a_{\underbrace{ij\ldots k}_{m}} |\underbrace{ij\ldots k}_{m}\rangle_{x_1x_2\ldots x_m}) \otimes \prod_{i'=1}^{m} [\frac{1}{2}(|000\rangle + |111\rangle)_{A_{1i'}B_{1i'}B_{2i'}} \otimes (|000\rangle + |111\rangle)_{A_{2i'}B_{3i'}C_{i'}}]. \qquad (16)$$

Alice can transfer the information of her unknown state into the particles controlled by her four agents by performing m GHZ-state measurements on her particles. That is, she takes a GHZ-state measurement on the particles x_i, A_{1i}, and A_{2i}, where i is the i-th particle in the unknown state or the i-th GHZ state shared with her agents. Three agents can act as the controllers and the other one acts as the receiver who can recover the unknown m-qubit state with the help of all the controllers. In this scheme, each of the controllers takes m single-particle measurements on his particles with the basis X, and tells the receiver his outcomes when they cooperate to recover the unknown state $|\xi\rangle_u$.

TABLE II: The relation between the values of V_i, P_i and the local unitary operations U_i.

V_i	0	0	1	1
P_i	+	−	+	−
U_i	I	σ_z	σ_x	$i\sigma_y$

The relation between the outcomes of measurements and the local unitary operations with which the receiver can recover the unknown state is shown in Table II. That is, Charlie can reconstruct the unknown state $|\xi\rangle$ according to the Table II if he cooperates with all the controllers. Here V_i is the value of the outcomes of the i-th GHZ-state measurement done by Alice. That is, $V_i = 0$ if Alice takes a GHZ-state measurement on the particles x_i, A_{1i}, and A_{2i}, and obtains the outcomes $\{|\Psi_0\rangle_{x_iA_{1i}A_{2i}}, |\Psi_1\rangle_{x_iA_{1i}A_{2i}}, |\Psi_4\rangle_{x_iA_{1i}A_{2i}}, |\Psi_5\rangle_{x_iA_{1i}A_{2i}}\}$; otherwise, $V_i = 1$. P_i is the product of the parities of all the outcomes in the i-th measurements done by Alice and her agents, i.e., $P_i = P_{A_i}P_{B_{1i}}P_{B_{2i}}P_{B_{3i}}$.

With the information published by Alice and the three controllers, the receiver, say Charlie, can recover the unknown state. In this time, Charlie need only take the unitary operation U_i on the i-th ($i = 1, 2, \cdots, m$) particle controlled by him. After m operations are performed on all his particles, Charlie obtains the unknown state $|\xi\rangle_u$. Same as the case for sharing a single-qubit state, this scheme for sharing m qubits is secure if the quantum channel, two sequences of three-particle GHZ states, is set up securely.

IV. DISCUSSION AND SUMMARY

As three-particle GHZ states are maximally entangled ones, the receiver Charlie can reconstruct the unknown m-qubit state $|\xi\rangle_u$ with the probability 100% in principle if he cooperates with all the other agents, same as Ref. [33]. Certainly, without the outcomes obtained by the three controllers, Charlie cannot recover the unknown state $|\xi\rangle_u$ even though he obtains the outcome published by Alice. On the one hand, Charlie does not know whether the controllers measure their particles with the basis X or not. That is, Charlie does not know whether his particles C_i still entangles with those controlled by the three controllers or not. On the other hand, Charlie does not know how to choose his unitary operations for recovering the unknown state even though he knows the fact that all the controllers have measured their particles but not the outcomes. That is, he will only has the probability $\frac{1}{2^m}$ to get the correct result if one of the three controllers does not agree to cooperate as Charlie has only half of the chance to choose the correct operation for each qubit C_i according to the information published by Alice and the other two controller, shown in Table II.

In detail, when Alice obtains the value $V_i = 0$, Charlie should choose one of the two unitary operations $\{I, \sigma_z\}$; otherwise, he should choose one of the other two unitary operations $\{\sigma_x, i\sigma_y\}$. Charlie can divide the four unitary operations into two groups according to the value V_i, but he cannot determine which one of two operations. In a word, without the help of the controllers, Charlie cannot reconstruct the originally unknown state $|\xi\rangle_u$. That is, the security of this QSTS scheme is the same as that of the quantum channel. As the quantum channel can be set up with decoy-photon technique [42] and multipartite entanglement purification [44], this QSTS is in principle secure. Also, Alice can exploit the faithful-qubit-transmission technique [45] to improve the efficiency for setting up the quantum channel in the condition with a collective noise.

In this five-party QSTS scheme, all the quantum sources (two sequence of GHZ states shared) can be used to carry the quantum information if all the agents act in concert after the quantum channel is set up securely with the decoy-photon technique [42] and the faithful-qubit-transmission technique [45]. The proportion of the decoy photons is small and can be neglectable in theory. That is, the intrinsic efficiency for qubits $\eta_q \equiv \frac{q_u}{q_t}$ in this QSTS scheme approaches 100%, same as all other QSTS schemes based on maximally entangled quantum channel [30–34]. Here q_u is the number of the useful qubits in QSTS and q_t is the number of qubits transmitted. The total efficiency η_t of QSTS schemes can be calculated as follows [33],

$$\eta_t = \frac{q_u}{q_t + b_t}, \tag{17}$$

where b_t is the number of the classical bits exchanged for sharing the unknown states. In this five-party QSTS scheme, $q_u = q_t = 4m$, and $b_t = 5m$ as Alice announces $2m$ bits of outcomes of the three-particle GHZ-state measurements and each of the three controllers tells the receiver m bits of outcomes of the measurements with the basis X. That is, $\eta_t = \frac{4}{9}$ which is the maximal value for QSTS [33], higher than that ($\frac{1}{3}$) in the QSTS scheme based on Bell states [30] in the case with four agents.

This five-party QSTS scheme for sharing an m-qubit state has some advantages. First, it only resorts to three-particle GHZ-state quantum channel, not a five-particle one as those in Refs. [11, 13, 31–39]. In practical, it is more convenient than some other QSTS schemes as it is more difficult for people to prepare five-particle entanglements than three-particle entanglements [46–48]. Secondly, the sender Alice need only perform three-particle GHZ-state measurements on her particles, not five-particle GHZ-state joint measurements as that in Ref. [30]. Thirdly, this QSTS scheme is in principle secure if the number of the dishonest agents is large than one (less than four). That is, it does not require that at most one of the agents is dishonest [40, 41]. Fourthly, the controllers need only take m single-particle measurements on their particles for completing the task of controlling. Moreover, this QSTS scheme is a symmetric one in which each of the agents can act as the receiver who can recover the unknown state with the help of the others. The amount of classical information exchanged in this scheme is less than others, and its total efficiency approaches the maximal value in theory.

Certainly, the QTS scheme shown in Ref. [30] uses Bell states as quantum channel for sharing a quantum information. If it is used for sharing an unknown state with four agents, the sender Alice should take a six-particle joint GHZ-state measurement on her particle. At the aspect of resource, the scheme [30] is simper than the present one. However, it requires six-particle joint GHZ-state measurements, which makes more difficult to be implemented at experiment than the present one. Also the second QSTS scheme in Ref.[39] exploits non-maximally two-particle entangled states as quantum channel, which makes it more convenient than the present one at the aspect of resource, similar to that in Ref.[30]. When it is used by the sender Alice to share a unknown state with her four agents, six-particle generalized GHZ-state measurements are required. At present, it is very difficult to prepare an entangled quantum system composed of more than four particles [46–48]. On the other hand, six-particle joint measurements are beyond what are available at experiment at present. With development of technique, those difficulties may be not the obstruct for implementing multiparty quantum state sharing efficiently.

In summary, we have presented an efficient and economic scheme for five parties to share an arbitrary m-qubit state with three-particle GHZ states, not five-particle ones. The sender Alice need only perform m three-particle joint measurements on her particles, not five-particle joint measurements, and each of the three controllers need only take m single-particle measurements on his particles with the basis X. These two factors make this QSTS scheme more convenient than others. As almost all the quantum resource can be used to share the quantum information and the classical information exchanged is minimal, the total efficiency in this scheme approaches the maximal value $\frac{4}{9}$. Moreover, this scheme is in principle secure even though there are more than one dishonest agents (less than four), different from that with two-photon entanglements and Bell-state measurements in Ref. [40].

This work is supported by the National Natural Science Foundation of China under Grant No. 10604008, A Foundation for the Author of National Excellent Doctoral Dissertation of China under Grant No. 200723, and Beijing Education Committee under Grant No. XK100270454.

[1] G. R. Blakley, in *Proceedings of the American Federation of Information Processing 1979 National Computer Conference* (American Federation of Information Processing, Arlington, VA, 1979), pp.313-317; A. Shamir, Commun. ACM **22**, 612 (1979)
[2] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
[3] F.G. Deng, G.L. Long, Phys. Rev. A **68**, 042315 (2003)
[4] F.G. Deng, G.L. Long, Phys. Rev. A **70**, 012311 (2004)
[5] G.L. Long, X.S. Liu, Phys. Rev. A **65**, 032302 (2002)
[6] H.K. Lo, H.F. Chau, M. Ardehali, J. Cryptology **18**, 122 (2005)
[7] F.G. Deng, G.L. Long, X.S. Liu, Phys. Rev. A **68**, 042317 (2003)
[8] F.G. Deng, G.L. Long, Phys. Rev. A **69**, 052319 (2004); Commun. Theor. Phys. **46**, 443 (2006)
[9] C. Wang et al., Phys. Rev. A **71**, 044305 (2005); C. Wang et al., Opt. Commun. **253**, 15 (2005); X.H. Li et al., Chin. Phys. **16**, 2149 (2007); X.H. Li et al., Phys. Rev. A **74**, 054302 (2006)
[10] F.G. Deng et al., Phys. Lett. A **359**, 359 (2006); F.G. Deng et al., Phys. Scr. **76**, 25 (2007); X.H. Li et al., Chin. Phys. Lett. **23**, 1080 (2006)
[11] M. Hillery, V. Bužek, A. Berthiaume, Phys. Rev. A **59**, 1829 (1999)
[12] A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A **59**, 162 (1999)
[13] L. Xiao et al., Phys. Rev. A **69**, 052307 (2004)
[14] D. Gottesman, Phys. Rev. A **61**, 042311 (2000)
[15] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000)
[16] V. Karimipour, A. Bahraminasab, S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002)
[17] C.P. Yang, J. Gea-Banacloche, J. Opt. B: Qantum Semiclass. Opt. **3**, 407, (2001)
[18] F.G. Deng et al., Chin. Phys. Lett. **23**, 1084 (2006); Phys. Lett. A 372, 1957 (2008)
[19] F.G. Deng et al., Phys. Lett. A **340**, 43 (2005); **354**, 190 (2006); Chin. Phys. Lett. **21**, 2097 (2004)
[20] P. Zhou et al., Physica A **381**, 164 (2007)
[21] P. Chen et al., Chin. Phys. **15**, 2228 (2006)
[22] F.G. Deng et al., Phys. Lett. A **337**, 329 (2005)
[23] Z.J. Zhang, Y. Li, Z.X. Man, Phys. Rev. A **71**, 044301 (2005)
[24] F.G. Deng et al., Phys. Rev. A **72**, 044302 (2005)
[25] F.L. Yan, T. Gao, Phys. Rev. A **72**, 012304(2005)
[26] F.G. Deng et al., J. Phys. A **39**, 14089 (2006)
[27] P. Zhou et al., Chin. Phys. Lett. **24**, 2181 (2007)
[28] R. Cleve, D. Gottesman, H.K. Lo, Phys. Rev. Lett. **83**, 648 (1999)
[29] A.M. Lance et al., Phys. Rev. Lett. **92** 177903 (2004); A.M. Lance et al., Phys. Rev. A **71**, 033814 (2005)
[30] Y.M. Li, K.S. Zhang, K.C. Peng, Phys. Lett. A **324**, 420 (2004)
[31] F.G. Deng et al., Phys. Rev. A **72**, 022338 (2005)
[32] F.G. Deng et al., Phys. Rev. A **72**, 044301 (2005)
[33] X.H. Li et al., J. Phys. B **39**, 1975 (2006)
[34] X.H. Li, F.G. Deng, H.Y. Zhou, Chin. Phys. Lett. **24**, 1151 (2007)
[35] C.Y. Cheung, Phys. Scr. **74**, 459 (2006)
[36] Z.X. Man, Y.J. Xia, N.B. An, Euro. Phys. J. D **42**, 333 (2007)
[37] Z.Y. Wang , H. Yuan, S.H. Shi, Z.J. Zhang, Eur. Phys. J. D **41**, 371 (2007)
[38] P. Zhou et al., J. Phys. A **40**, 13121 (2007).
[39] G. Gordon, G. Rigolin, Phys. Rev. A **73**, 062316 (2006)
[40] F.G. Deng et al., Eur. Phys. J. D **39**, 459 (2006).
[41] Y.Q. Zhang, X.R. Jin, S. Zhang, Chin. Phys. 15 (2006) 2252.
[42] C.Y. Li et al., Chin. Phys. Lett. **22**, 1049 (2005); C.Y. Li et al., Chin. Phys. Lett. **23**, 2896 (2006); X.H. Li et al., J. Korean Phys. Soc. **49**, 1354 (2006).
[43] F.G. Deng, X.H. Li, H.Y. Zhou, arXiv:0705.0279.
[44] M. Murao et al., Phys. Rev. A 55 (1998) 2839.
[45] X.H. Li, F.G. Deng, H.Y. Zhou, Appl. Phys. Lett. **91**, 144101 (2007).
[46] D. Bouwmeester, J.W. Pan, M. Daniell, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999)
[47] J.W. Pan et al., Phys. Rev. Lett. **86**, 4435 (2001)
[48] Z. Zhao et al., Nature (London) **430**, 54 (2004).